COVID-19: NO IMPACT ON 1 JULY ENFORCEMENT DATE SET FOR CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA)

Date: 31 March 2020

U.S. Privacy Alert

By: Tara C. Clancy, Paul W. Sweeney, Jr.

Despite over 60 business groups asking the California Attorney General (AG) to delay the enforcement of the CCPA in light of the COVID-19 pandemic, the AG's office has stated there are no plans to delay the 1 July enforcement date. Complicating matters further, the third draft of the CCPA-related regulations (which aim to interpret and implement the CCPA) were open for comment until 27 March and are not yet final. Each draft, to date, has contained material and substantial changes. Additionally, in light of COVID-19, many businesses' data collection practices have changed to accomplish screening and safe work environments, and these practices may impact what should be included in privacy notices.

The risk of noncompliance is significant. The AG may bring an enforcement action for any violation of the CCPA. After notice, a business has 30 days to cure the alleged violation or be subject to civil penalties up to $2,500 for each violation ($7,500 if intentional). In these times when business operations have shifted to a digital platform, those numbers can add up quickly. Notably, the current regulations offer no guidance on what will constitute a "cure." In an interview with Reuters on 10 December 2019, the AG stated that "[w]e will look kindly on those that … demonstrate an effort to comply" but will "make an example of" businesses that fail to comply.[1]

In this changing setting, the following are some points to consider in managing CCPA compliance.

CONSIDERATIONS FOR COMPLIANCE

1. **Review and update your privacy notices:** Do your current notices accurately reflect your data collection practices?
    - Have you changed your data collection practices due to COVID-19? For example, if you are engaged in screening employees for COVID-19, you may need to update your internal notification policy to cover what categories of information are being collected and describe the business purpose(s) for use.
    - Consider any application to on-site visitors of your premises, including job applicants and contractors.
2. **Check your processes for handling consumer requests:** Current regulations require confirmation of requests to know or requests to delete within 10 business days and then processing such requests within 45 calendar days.
    - Has a remote work force impacted your ability to timely access and process requests, including verification? Have furloughs had (or will sick leave have) a similar impact? While there is the ability to

take one 45 calendar day extension, you must notify the consumer that you are taking the extension within the first 45 day period and provide an explanation of the reason for taking the extension. Consider drafting appropriate language for those notifications now.

- Do you have the appropriate "review" mechanisms in place before sending copies of information to a consumer to avoid mishandling the data and creating a breach?
- Is there a need for additional training of employees handling requests, and can you accomplish this training through virtual resources?

3. **Confirm your "Do Not Sell My Personal Information" link is CCPA compliant:** If your business sells information, confirm you have a "Do Not Sell My Personal Information" link on your website homepage (or app landing page) that directs consumers to a notice of their opt-out rights.
   - Can your business comply with any request to opt out within 15 business days?
   - Do you have the appropriate contact points for any third parties that have been sold information given the shift to remote workforces?
4. **Think security:** It is common for data incidents to increase during uncertain times. Make sure your information technology systems are robust and updates are timely made. Under the CCPA, a failure to implement and maintain "reasonable security" practices can expose a business to statutory damages in the event of a data breach.
   - Are you regularly assessing risks, particularly risks associated with a remote workforce, and modifying practices based on such assessments?
   - Have you reviewed your incident response plan to make sure it addresses an effective incident response in an environment where it is not "business as usual"?
   - Consider encryption and redaction of certain personal information to mitigate litigation risks, namely, the personal information defined under Cal. Civ. Code § 1798.81.5(d)(1) (e.g., an individual's name in combination with a Social Security number, state identification, account number and security code, medical information, health insurance information, biometric information, or username/email address in combination with password/security question and answer, which would permit access to an online account). A consumer cannot bring a private right of action where only redacted or encrypted information is subject to a breach.
5. **Consider cyber insurance:** If you already have a cyber policy, have you reviewed its terms in light of the potential liability from either an enforcement action by the AG's office or a private right of class action due to a breach?
   - What are your current limits in view of potential exposure?
   - How is personal information defined in your policy? Does it take into account the broader definition in the CCPA?
   - Is your policy limited by an intentional acts exclusion (e.g., a fine levied by the AG's office for an "intentional violation") or is coverage conditioned on insurability under applicable law, which may prohibit coverage for the payment of a fine (see Insurance Code § 533.5).

CONCLUSION

Despite the current disruptions due to COVID-19, businesses must be in compliance or moving toward full compliance with the CCPA. Consider assembling CCPA compliance teams to review current policies and notices and discuss and prioritize action plans. If compliance teams have made a good-faith effort to comply, even during the challenges presented by COVID-19, and have records of their compliance efforts, it is less likely they will be viewed as an egregious offender warranting an enforcement action and severe penalties.

FOOTNOTES

[1] There is also the risk of private plaintiffs using the California Unfair Competition Law (UCL) to enforce violations of the CCPA. While it is unlikely that the California legislature intended the UCL to be used as a backdoor to enforce the CCPA, based on the CCPA (i) stating the private right of action applies only to data breaches, and (ii) providing the AG with enforcement authority, one class action alleging a violation of the UCL based on failing to provide notice under the CCPA prior to collecting biometric data has been filed in the Southern District of California. See Burke v. Clearview AI, Inc., Case No. 3:20-cv-00370 (S.D. Cal. 27 Feb. 2020).

KEY CONTACTS

TARA C. CLANCY
PARTNER

BOSTON
+1.617.261.3121
TARA.CLANCY@KLGATES.COM

PAUL W. SWEENEY, JR.
PARTNER

LOS ANGELES
+1.310.552.5055
PAUL.SWEENEY@KLGATES.COM

